

FILED ENTERED  
LODGED RECEIVED

FEB 11 2011

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTY  
BY

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

IN THE MATTER OF THE UNITED STATES OF  
AMERICA'S APPLICATION FOR A SEARCH  
WARRANT TO SEIZE AND SEARCH ELECTRONIC  
DEVICES FROM EDWARD CUNNIUS

Case No. **MJ11-55**  
MEMORANDUM ORDER DENYING  
THE GOVERNMENT'S APPLICATION  
FOR A WARRANT TO SEIZE AND  
SEARCH ELECTRONIC DEVICES

SEALED ORDER

I. INTRODUCTION AND SUMMARY CONCLUSION

This matter comes before the Court on the government's application for a warrant to search the residence of Edward Cunnus, to seize any computers or digital devices (collectively "digital devices")<sup>1</sup> that may be located at the premises, and to search all electronically stored information ("ESI") contained in any digital devices seized from Mr. Cunnus' residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods. Specifically, in addition to the search of the residence and the seizure of digital devices, the application requests the authority for investigative officers to: (1) search all ESI contained in Mr. Cunnus' digital devices and related to the use of the devices; (2) conduct the search without segregation by a filter team; (3) conduct the search without foreswearing the plain view doctrine;

<sup>1</sup> "Digital devices" is defined in the warrant affidavit to include any electronic device capable of processing or storing data in digital form. Larson Aff. ¶ 37 n.1; Larson Warrant App., Att. B, ¶ 2.

1 and (4) permit investigative agents to obtain a second warrant if, during the search of the ESI, the  
2 investigating and searching agents find evidence of crime outside the scope of the instant  
3 warrant. On February 7, 2011, the Court advised the Assistant United States Attorney  
4 (“AUSA”) that the warrant, as presented, would not be granted. The United States has refused to  
5 accede to the Court’s view that a filter team and forswearing reliance on the plain view doctrine  
6 are appropriate, and indeed, required in this specific case. Accordingly, the AUSA requested the  
7 Court to file a memorandum opinion, so that the government can appeal. A copy of the  
8 requested warrant and affidavit in support is attached as Exhibit 1. That request has led to this  
9 opinion.

10 Because the government, in this application, refuses to conduct its search of the digital  
11 devices utilizing a filter team and forswearing reliance on the plain view doctrine, the Court  
12 DENIES the application as seeking an overbroad or general warrant in violation of the Fourth  
13 Amendment and the law of this Circuit.<sup>2</sup>

## 14 II. DISCUSSION

### 15 A. *The Warrant Application to Seize and Search ESI devices*

16 The affidavit in support of the government’s warrant application indicates that agents  
17 received information from Microsoft Corporation (“Microsoft”) in October 2010 regarding an  
18 individual, Mr. Cunnius, whom they believed was advertising counterfeit Microsoft software via  
19 the internet classified advertising service Craigslist. Specifically, a Microsoft anti-piracy  
20 investigator informed agents that a shipment of counterfeit Microsoft software from China,

---

21  
22 <sup>2</sup> The Court is prepared to authorize the search of the residence. This opinion focuses on the  
23 search of digital devices contained in the residence. There are other changes to the warrant regarding  
hash values that would be required, as discussed in Part II Section E of this opinion. The Court does not  
understand the government to have objections to these changes, but if this is not the case, the government  
should address the issue in its appeal.

1 addressed to "Edward Russell Cunnus" at 2305 Rucker Avenue #5, Everett, Washington, had  
2 been seized by Customs and Border Protection ("CBP") on October 18, 2010. In response to the  
3 CBP seizure, Microsoft sent a warning letter advising Mr. Cunnus that it had received  
4 information that he or someone with his company may have distributed illegal and/or unlicensed  
5 Microsoft software. The letter informed Mr. Cunnus of the consequences of illegal distribution.

6 The Microsoft investigator also informed the agents that Mr. Cunnus was responsible for  
7 numerous Craigslist advertisements over the past few months that offered to sell brand new, in-  
8 the-box, Microsoft software at prices well below typical retail prices for the same software.  
9 After contacting Mr. Cunnus at the phone number listed on the Craigslist advertisements,  
10 Microsoft conducted an undercover test purchase of several products from Mr. Cunnus at his  
11 home in Everett, Washington. These products were purchased at prices substantially below retail  
12 value, and upon further examination, were found to be counterfeit.

13 Following Microsoft's test purchase, undercover law enforcement agents conducted two  
14 test purchases from Mr. Cunnus at his apartment. On each occasion, agents contacted Mr.  
15 Cunnus via the telephone number listed in his Craigslist advertisements, and met with Mr.  
16 Cunnus at his apartment. The agents purchased several boxes of purportedly genuine, new, in-  
17 the-box, Microsoft software from Mr. Cunnus on December 13, 2010, and December 21, 2010,  
18 respectively. During each purchase, Mr. Cunnus retrieved the boxes containing the software  
19 from a closet in the bedroom of his apartment. According to the affidavit, he was evasive in  
20 response to questions regarding the authenticity of the products, and stated that if customers  
21 complained to him, he would instruct them to go buy the products for much higher prices at retail  
22 establishments. The agents submitted the products purchased from Mr. Cunnus to Microsoft for  
23 analysis by their product identification specialists, who determined that the products were

1 counterfeit.

2 In response to questions regarding Mr. Cunnius' supplier, Mr. Cunnius told the  
3 undercover agents that it took him years to make his contact with his supplier and that he  
4 receives his product through the mail. He also told the agents that he communicates with his  
5 source via electronic mail, and pays him through electronic transfer from his bank.

6 The government then applied to this Court for a warrant authorizing agents to search Mr.  
7 Cunnius' apartment and seize evidence, fruits and instrumentalities of the crimes of (1) copyright  
8 infringement and/or (2) trafficking in counterfeit goods. Specifically, the government believes  
9 that evidence related to how Mr. Cunnius obtained counterfeit software, paid for it, and how he  
10 distributed the counterfeit software is likely to be discovered on digital devices located at his  
11 apartment. This evidence may include e-mail correspondence with Mr. Cunnius' source,  
12 evidence of internet banking transactions, and evidence of his online advertisements and  
13 marketing of counterfeit software. In addition, the government wishes to search for evidence of  
14 dominion and control of any digital device located in the apartment in order to determine who  
15 else may be responsible for obtaining and trafficking in the counterfeit software purchased from  
16 Mr. Cunnius, and who may have been using the computers at the relevant time.

17 There is no suggestion that the target is using the digital devices to "burn" counterfeit  
18 discs, or to transmit counterfeit copies electronically. Instead, the target of the investigation  
19 allegedly sells in-the-box counterfeit copies that have been imported.

20 The Court finds that the warrant affidavit establishes probable cause to search the digital  
21 devices located at Mr. Cunnius' residence for evidence of criminal copyright infringement and/or  
22 trafficking in counterfeit goods. Probable cause exists if "it would be reasonable to seek the  
23 evidence in the place indicated in the affidavit." *United States v. Wong*, 334 F.3d 831, 836 (9th

1 Cir. 2003) (quoting *United States v. Peacock*, 761 F.2d 1313, 1315 (9th Cir. 1985)). The two  
2 crimes contemplated by the warrant in this case involve the “distribution” or “trafficking” of  
3 certain goods. Specifically, criminal copyright infringement includes “willfully infring[ing] a  
4 copyright” if that infringement was committed “for purposes of commercial advantage or private  
5 financial gain . . . by the reproduction or distribution, including by electronic means . . . of 1 or  
6 more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of  
7 more than \$1,000.” 17 U.S.C. § 506(a), (b). Similarly, trafficking in counterfeit goods involves  
8 “intentionally traffic[king] or attempt[ing] to traffic in goods or services and knowingly us[ing] a  
9 counterfeit mark on or in connection with such goods or services . . . the use of which is likely to  
10 cause confusion, to cause mistake, or to deceive. . . .” 18 U.S.C. § 2320(a), (b). In light of the  
11 sworn affidavit that Mr. Cunnius advertises the counterfeit goods by posting advertisements  
12 containing digital photographs of the products on the website Craigslist, communicates with his  
13 source by e-mail, and pays his source using electronic transfers from his bank, the Court can  
14 reasonably assume that digital devices contain evidence relating to the crimes alleged.

15       However, despite the existence of probable cause to search the digital devices, the Court  
16 finds the warrant requested by the government overbroad. The affidavit contains no reference to  
17 use of a filter team, and no promise to forswear reliance on the plain view doctrine. With  
18 respect to the procedures to be employed by law enforcement personnel to execute the search of  
19 digital devices, once they have been seized, the affidavit provides:

20               In order to examine the ESI in a forensically sound manner, law  
21 enforcement personnel with appropriate expertise will produce a  
22 complete forensic image, if possible and appropriate, of any digital  
23 device that is found to contain data or items that fall within the  
scope of Attachment B of this Affidavit. In addition, appropriately  
trained personnel may search for and attempt to recover deleted,  
hidden, or encrypted data to determine whether the data fall within  
the list of items to be seized pursuant to the warrant. In order to

1 search fully for the items identified in the warrant, law  
2 enforcement personnel may then examine all of the data contained  
3 in the forensic image/s and/or on the digital devices to view their  
precise contents and determine whether the data falls within the list  
of items to be seized pursuant to the warrant.

4 The search techniques that will be used will be only those  
5 methodologies, techniques and protocols as may reasonably be  
6 expected to find, identify, segregate, and/or duplicate the items  
authorized to be seized pursuant to Attachment B to this affidavit.

7 If, after conducting its examination, law enforcement personnel  
8 determine that any digital device is an instrumentality of the  
9 criminal offense referenced above, the government may retain that  
10 device during the pendency of the case as necessary to, among  
11 other things, preserve the instrumentality evidence for trial, ensure  
the chain of custody, and litigate the issue of forfeiture. If law  
enforcement personnel determine that a device was not an  
instrumentality of the criminal offense referenced above, it shall be  
returned to the person/entity from whom it was seized within 90  
days of the issuance of the warrant, unless the government seeks  
and obtains authorization from the court for its retention.

12 Unless the government seeks an additional order of authorization  
13 from any Magistrate Judge in the District, the government will  
14 return any digital device that has been forensically copied, that is  
15 not an instrumentality of the crime, and that may be lawfully  
possessed by the person/entity from whom it was seized, to the  
person/entity from whom it was seized within 90 days of seizure.

16 If, in the course of their efforts to search the subject digital devices,  
17 law enforcement agents or analysts discover items outside of the  
18 scope of the warrant that are evidence of other crimes, that  
19 data/evidence will not be used in any way unless it is first  
20 presented to a Magistrate Judge of this District and a new warrant  
is obtained to seize that data, and/or to search for other evidence  
related to it. In the event a new warrant is authorized, the  
government may make use of the data then seized in any lawful  
manner.

21 Larson Aff. ¶ 46(c)-(g).

22 As discussed below, permitting the government to conduct a search along  
23 these lines would violate the Fourth Amendment and the law of this Circuit.



1           B.       *The Fourth Amendment Prohibits General Searches*

2           The instant warrant application cannot be squared with the Fourth Amendment's  
3 prohibition on general searches. The Fourth Amendment states:

4                   The right of the people to be secure in their persons, houses,  
5 papers, and effects, against unreasonable searches and seizures,  
6 shall not be violated, and no Warrants shall issue, but upon  
7 probable cause, supported by Oath or affirmation, and particularly  
8 describing the place to be searched, and the persons or things to be  
9 seized.

10           U.S. Const. amend. IV. The Warrant Clause of the Fourth Amendment categorically prohibits  
11 the issuance of any warrant except one "particularly describing the place to be searched and the  
12 persons or things to be seized." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (citing U.S.  
13 Const. amend. IV). As the Supreme Court noted:

14                   [t]he manifest purpose of this particularity requirement was to  
15 prevent general searches. By limiting the authorization to search to  
16 the specific areas and things for which there is probable cause to  
17 search, the requirement ensures that the search will be carefully  
18 tailored to its justifications, and will not take on the character of  
19 the wide-ranging exploratory searches the Framers intended to  
20 prohibit.

21           *Id.* This understanding of the Fourth Amendment's particularity requirement broke no new  
22 ground. Indeed, sixty years before *Maryland v. Garrison* was decided, the Supreme Court  
23 recognized general searches were long deemed to violate the Constitution. *Marron v. U.S.*, 275  
U.S. 192, 196 (1927).

          The Fourth Amendment's particularity provision was enacted to respond to the evils of  
general warrants and writs of assistance which English judges had employed against the  
colonists. *Virginia v. Moore*, 553 U.S. 164, 169 (2008). As the Supreme Court stated:

          The practice had obtained in the colonies of issuing writs of  
assistance to the revenue officers, empowering them, in their  
discretion, to search suspected places for smuggled goods, which

1 James Otis pronounced “the worst instrument of arbitrary power,  
2 the most destructive of English liberty and the fundamental  
3 principles of law, that ever was found in an English law book;”  
since they placed “the liberty of every man in the hands of every  
petty officer.”

4 *Boyd v. United States*, 116 U.S. 616, 625 (1886) (internal footnotes omitted). The requirement  
5 was thus designed to ensure only a specific place is searched and that probable cause to search  
6 that place actually exists. *See Steele v. United States*, 267 U.S. 498, 501-02 (1925).<sup>3</sup>

7 Here, the government seeks permission to search every bit of data contained in each  
8 digital device seized from Mr. Cunnius’ residence. Contrary to the Fourth Amendment’s  
9 particularity requirement limiting searches to only the specific areas and things for which there is  
10 probable cause to search, the government seeks to scour everything contained in the digital  
11 devices and information outside of the digital devices. This practice is akin to the revenue  
12 officers in colonial days who scoured “suspected places” pursuant to a general warrant.

13 The Court has considered the fact that the search warrant application seeks permission to  
14 search and seize evidence of the specified crimes, and a second warrant would be needed to seize  
15 evidence of other crimes for which there is no probable cause shown. However, the ability to  
16 seek a second warrant after finding evidence as to which there was no probable cause to search  
17 only magnifies the danger of the warrant constituting a general warrant. The requirement that a  
18 second warrant be obtained provides no meaningful limitation on the scope of the search  
19 conducted under the first warrant and no meaningful protection against the government obtaining  
20 evidence for which it lacks probable cause. For the first warrant would be nothing more than a

---

21  
22 <sup>3</sup> The Fourth Amendment’s prohibition on the issuance of general warrants goes hand in hand  
23 with the requirement that each search must be carefully tailored to its justifications. Hence, even if a  
warrant is not an impermissible general warrant, it still cannot be granted unless it is carefully tailored to  
its justification.



1 “vehicle to gain access to data for which the government has no probable cause to collect.”

2 *Comprehensive Drug Testing v. United States*, 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc)

3 (“*CDT III*”).<sup>4</sup> Indeed, the warrant the government now seeks would permit it to seize evidence

4 found outside the scope of the first warrant whether that evidence was initially in plain view, or

5 not.

6 C. *What is Involved in a Digital Search?*

7 As noted above, there is no suggestion in the affidavit that the digital devices at issue are

8 being used to burn counterfeit discs or otherwise create or electronically transmit illegal copies

9 of the software at issue. Instead, the affidavit makes it clear that the allegedly counterfeit

10 software at issue is being imported. The search of the digital devices would undoubtedly be

11 helpful to reveal the source(s) of supply, the quantity, customer names of the counterfeit

12 merchandise, financial gains from the activity, and knowledge of the counterfeit nature of the

13 goods. Against these legitimate needs, the Court weighs the vast amount and nature of data that

14 can be stored on or accessed by personal computers, an analysis which illustrates the continued

15 importance of the Fourth Amendment’s particularity requirement.

16 1. *A Digital Search Captures Vast Quantities of Data*

17 A government search of even a single, non-networked computer involves searching vast

18 quantities of ESI. As pointed out in the warrant affidavit, a single gigabyte of storage space is

19 the equivalent of 500,000 double-spaced pages of text. *Larson Aff.* ¶ 45(b). Computer hard

---

20  
21 <sup>4</sup> The Ninth Circuit’s initial panel decision is found at *Comprehensive Drug Testing v. United*  
22 *States*, 473 F.3d 913 (9th Cir. 2006). This panel decision was withdrawn and superseded by  
23 *Comprehensive Drug Testing v. United States*, 513 F.3d 1085 (9th Cir. 2008) (“*CDT I*”). The Ninth  
Circuit then granted rehearing *en banc*, *Comprehensive Drug Testing v. United States*, 545 F.3d 1160 (9th  
Cir. 2008), and issued its first *en banc* decision at *Comprehensive Drug Testing v. United States*, 579 F.3d  
989 (9th Cir. 2009) (“*CDT II*”). The initial *en banc* decision was then revised and superseded by *CDT III*,  
621 F.3d 1162.

1 drives are now being sold for personal computers capable of storing up to two terabytes, or 2,048  
2 gigabytes of data. *Id.* If a computer is networked, this exponentially increases the volume of  
3 data being searched. Thus, the sheer volume of ESI involved distinguishes a digital search from  
4 the search of, for example, a file cabinet.

5 2. *A Digital Search Captures Innocent and Personal Information With*  
6 *No Relevance to the Asserted Crimes*

7 Because it is common practice for people to store innocent and deeply personal  
8 information on their personal computers, a digital search of ESI will also frequently involve  
9 searching personal information relating to the subject of the search as well as third parties. As  
10 Judge Kleinfeld noted:

11 The importance of this case is considerable because, for most  
12 people, their computers are their most private spaces. People  
13 commonly talk about the bedroom as a very private space, yet  
14 when they have parties, all the guests - including perfect strangers -  
are invited to toss their coats on the bed. But if one of those guests  
is caught exploring the host's computer, that will be his last  
invitation.

15 There are just too many secrets on people's computers, most legal,  
16 some embarrassing, and some potentially tragic in their  
17 implications, for loose liberality in allowing search warrants.  
18 Emails and history links may show that someone is ordering  
19 medication for a disease being kept secret even from family  
20 members. Or they may show that someone's child is being  
21 counseled by parents for a serious problem that is none of anyone  
22 else's business. Or a married mother of three may be carrying on a  
23 steamy email correspondence with an old high school boyfriend.  
Or an otherwise respectable, middle-aged gentleman may be  
looking at dirty pictures. Just as a conscientious public official  
may be hounded out of office because a party guest found a  
homosexual magazine when she went to the bathroom at his house,  
people's lives may be ruined because of legal but embarrassing  
materials found on their computers. And, in all but the largest  
metropolitan areas, it really does not matter whether any formal  
charges ensue - if the police or other visitors find the material, it  
will be all over town and hinted at in the newspaper within a few  
days.

Nor are secrets the only problem. Warrants ordinarily direct seizure, not just search, and computers are often shared by family members. Seizure of a shared family computer may, though unrelated to the law enforcement purpose, effectively confiscate a professor's book, a student's almost completed Ph.D. thesis, or a business's accounts payable and receivable.

*U.S. v. Gourde*, 440 F.3d 1065, 1077 (9th Cir. 2006) (Kleinfeld, J., dissenting).

### 3. *Digital Devices Function as a Portal in the Age of Cloud Computing*<sup>5</sup>

The language in the instant warrant raises another significant constitutional concern related to the interactive nature of modern digital devices. These digital devices are not just repositories of data, but access points, or portals, to other digital devices and data, typically obtained through the internet or stored on a network. All data on the internet is both separate and one. The requested warrant is, in essence, boundless. This is made evident by the fact that the government seeks authorization, among other things, to obtain "all passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data." *Larson Aff.* ¶ 47(g).

This poses a multitude of problems, and it highlights the concerns raised by Judge Kleinfeld. First, once the government has all passwords, it is able to access a defendant's most sensitive information. To the extent the defendant may have medical records on-line, that information is now available to the government. If the defendant's wife, who is not alleged to be involved in any criminal activity, is sending embarrassing, private e-mail messages, that

---

<sup>5</sup> "The term 'cloud computing' is based on the industry usage of a cloud as a metaphor for the ethereal internet. A cloud platform can either be external or internal. An external cloud platform is storage or software access that is essentially rented from (or outsourced to) a remote public cloud service provider, such as Amazon or Google. This software-as-a-service allows individuals and businesses to collaborate on documents, spreadsheets, and more, even when the collaborators are in remote locations. By contrast, an internal or private cloud is a cluster of servers that is networked behind an individual or company's own firewall." David A. Couillard, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2216 (2009) (internal citations omitted).

1 information is now available for use by the government. If the government wants to see what  
2 books the defendant is reading, or what movies his wife is viewing, all of this would be fair game  
3 under the warrant presented by the government. Moreover, if the defendant has been looking at  
4 legal but “dirty” pictures the government will know this as well, even if the defendant had  
5 intended to “throw them away.” The government candidly acknowledges that its protocols “are  
6 exacting scientific procedures designed to protect the integrity of evidence and recover even  
7 hidden, erased, compressed, password-protected, or encrypted files.” Larson Aff. ¶ 45.

8 4. *A Digital Search Captures ESI of Which the User Is Unaware*

9 In addition to granting the government access to ESI that was consciously downloaded by  
10 computer users, this boundless search would reveal ESI that computer users have no way of  
11 knowing is stored on their device.<sup>6</sup> A search of a file cabinet, in contrast, would include only  
12 items put in the file cabinet by a person. A conscious, even if unknowing, act is required. This  
13 act perhaps would be analogous to intentionally downloading a file. However, in contrast to the  
14 conscious act of downloading a file or storing something in a file cabinet, cache files are a set of  
15 files automatically stored on a user’s hard drive by a web browser to speed up future visits to the  
16 same websites, without the affirmative action of downloading. *See U.S. v. Romm*, 455 F.3d 990,  
17 993 n.1 (9th Cir. 2006). *See also U.S. v. Parish*, 308 F.3d 1025, 1030-31 (9th Cir. 2002). “Most  
18 web browsers keep copies of all the web pages that you view up to a certain limit, so that the  
19 images can be redisplayed quickly when you go back to them.” *Romm*, 455 F.3d at 993 n.1.  
20 Thus, a person’s entire online viewing history can be retrieved from the cache, without any  
21 affirmative act other than visiting a web page.

22  
23 <sup>6</sup> The Ninth Circuit has defined “downloading” as “the act of manually storing a copy of an image  
on the hard drive for later retrieval.” *U.S. v. Romm*, 455 F.3d 990, 994 n.3 (9th Cir. 2006). *See also U.S.*  
*v. Mohrbacher*, 182 F.3d 1041, 1045-46 (9th Cir. 1999) (describing downloading).

1           5.       *A Digital Search Captures "Destroyed" Data*

2           Unlike information in a file cabinet that can simply be taken out and destroyed, ESI is  
 3 present after attempts to destroy it. In addition to data stored in cache files, ESI can be recovered  
 4 from "unallocated space" on a hard drive, which "contains deleted data, usually emptied from the  
 5 operating system's trash or recycle bin folder, that cannot be seen or accessed by the user  
 6 without the use of forensic software." *United States v. Flyer*, No. 08-10580, slip op. at 2429 (9th  
 7 Cir. Feb. 8, 2011). The government knows that once ESI is created, it is very difficult to destroy,  
 8 and indeed, the government highlights this function. In the affidavit, the government states

9                       Once created, electronically stored information ("ESI") can be  
 10 stored for years in very little space and at little or no cost. A great  
 11 deal of ESI is created, and stored, moreover, even without a  
 12 conscious act on the part of the device operator. For example, files  
 13 that have been viewed via the Internet are sometimes automatically  
 14 downloaded into a temporary Internet directory or "cache,"  
 15 without the knowledge of the user. The browser often maintains a  
 fixed amount of hard drive space devoted to these files, and files  
 are only overwritten as they are replaced with more recently  
 viewed Internet pages or if a user takes steps to delete them. . . .  
 Even when such action [the affirmative attempts to delete] has  
 been deliberately taken, ESI can often be recovered, months or  
 even years later, using forensic tools.

16 Larson Aff. ¶ 44(a).

17           Although the probative evidence stored in any digital device seized in this case would  
 18 seem to be limited to the supplier(s), possible customers, warnings, and the underlying financial  
 19 data, the government has indicated that it may "search for and attempt to recover deleted, hidden,  
 20 or encrypted data 'to determine whether the data fall within the list of items to be seized.'"

21 Larson Aff. ¶ 46(c). Such a request sweeps into the search of a single ESI device all sites, all  
 22 data, and all persons that device accessed via the internet.  
 23

1           6.       *General Principles of the Fourth Amendment*

2           In opposing the requirement of a filter team and forswearing reliance on the plain view  
3 doctrine, the government has taken the position that the characteristics set forth above relating to  
4 digital searches do not require heightened Fourth Amendment protection, citing the U.S.  
5 Supreme Court's assertion in *Katz v. United States* that "the Fourth Amendment protects people,  
6 not places." 389 U.S. 347, 351 (1967). It contends that a digital search is no more intrusive than  
7 a properly authorized search that requires officers to sift through all of an individual's papers,  
8 and every possible place where such papers might be found within the home. The government  
9 also cites the Ninth Circuit's statement in *United States v. Giberson* that "[w]hile it is true that  
10 computers can store a large amount of material, there is no reason why officers should be  
11 permitted to search a room full of filing cabinets or even a person's library for documents listed  
12 in a warrant but should not be able to search a computer." 527 F.3d 882, 888 (9th Cir. 2008).

13           Following *Giberson*, however, the Ninth Circuit began to refine its analysis. In *U.S. v.*  
14 *Payton*, the court explained that "*Giberson* held that computers were not entitled to a special  
15 categorical protection of the Fourth Amendment. Instead, they remained subject to the Fourth  
16 Amendment's overall requirement that searches be constitutionally 'reasonable.'" 573 F.3d 859,  
17 863-64 (9th Cir. 2009). Under *Giberson*, "[i]f it is reasonable to believe that a computer contains  
18 items enumerated in the warrant, officers may search it." *Id.* at 864 (citing *Giberson*, 527 F.3d at  
19 888). With respect to the actual search conducted by the agents, however, the *Payton* court  
20 observed that "the nature of computers makes such searches so intrusive that affidavits seeking  
21 warrants for the search of computers often include a limiting search protocol, and judges issuing  
22 warrants may place conditions on the manner and extent of such searches, to protect privacy and  
23 other important constitutional interests . . . *We believe that it is important to preserve the option*



1 of imposing such conditions when they are deemed warranted by judicial officers authorizing the  
2 search of computers.” *Id.* at 864 (emphasis added). The *Payton* court concluded that “the  
3 special considerations of reasonableness involved in the search of computers are reflected by the  
4 practice, exemplified in *Giberson*, of searching officers to stop and seek an explicit warrant when  
5 they encounter a computer that they have reason to believe should be searched.” *Id.* As  
6 discussed further below, this refinement continued in the *CDT* line of cases.

7 D. *Comprehensive Drug Testing Inc. v. United States*

8 The unconstitutionality of the instant warrant application, as well as the application  
9 presented in *CDT III*, is revealed by tracing the odyssey of the *CDT* litigation. Here, the  
10 government seeks to search all data contained in digital devices seized from Mr. Cunnius’  
11 residence, as well as information outside the devices. The government intends to perform this  
12 search without a filter team to separate from the investigative agents information that is outside  
13 the scope of the warrant. Additionally, the warrant does not forswear reliance on the plain view  
14 doctrine, and further seeks authorization to obtain and use information found outside the scope of  
15 the initial warrant whether or not that information was found in plain view.

16 With this background, the Court turns to the Ninth Circuit opinion in *CDT III*. In that  
17 case, the government obtained a warrant to search CDT’s facilities limited to the records of ten  
18 baseball players for whom there was probable cause to suspect of drug use. Included in the  
19 warrant was a provision to allow seizure of computer records from CDT facilities for off-site  
20 examination and segregation of the evidence. To justify this provision, which the government  
21 acknowledged included information beyond that relevant to the investigation, the supporting  
22 affidavit contained information about the difficulty and hazards of retrieving only ESI for which  
23 the government had probable cause.

1 Based on these representations, a magistrate judge granted the government permission to  
2 engage in a broad seizure. However, the warrant the magistrate judge authorized also contained  
3 important restrictions on the handling of seized data, including review and segregation by non-  
4 investigating law enforcement personnel rather than the case agents. The purpose of the  
5 segregation requirement was to prevent case agents from accessing information outside the scope  
6 of the warrant.

7 Utilizing this warrant, agents found at CDT's facilities the "Tracey Directory," which  
8 included, among hundreds of other documents, a spreadsheet containing the names of all the  
9 major league baseball players who had tested positive for steroids.<sup>7</sup> The government had  
10 probable cause to search and seize records of ten baseball players. After deciding it was  
11 impractical to sort through the information on-site, the agents removed the data for off-site  
12 review. Although the warrant required segregation and screening, the case agent ignored this  
13 requirement and took control of the data.

14 Based on its search of the Tracey Directory, the government obtained additional warrants  
15 to search the facilities of CDT and Quest for information regarding more baseball players who  
16 they discovered had tested positive for steroids, and issued subpoenas demanding production of  
17 the same records it had just seized. The government claimed it was justified in obtaining this  
18 additional incriminating information, based on the plain view doctrine of evidence found outside  
19 the scope of the warrant. In response, CDT and the baseball players' association moved for  
20 return of the seized property.

21  
22  
23  

---

<sup>7</sup> Some of these baseball players were included in the warrant, some were not.

1 The litigation in *CDT III* involved multiple district courts. Two district courts ordered  
2 the government to return the property.<sup>8</sup> The judges expressed grave dissatisfaction with the  
3 government's conduct; some accused the government of manipulation and misrepresentations.  
4 As one district judge stated in rejecting the government's arguments, "whatever happened to the  
5 Fourth Amendment? Was it . . . repealed somehow?" *CDT III*, 621 F.3d at 1177 (citing *CDT I*,  
6 513 F.3d at 1117).

7 The government appealed to the Ninth Circuit. In a reissued decision, the panel reversed  
8 two of the district courts' orders to return the property, and held the government was bound by  
9 the third court's order containing factual determinations including the government's failure to  
10 comply with the warrant and that it had displayed a callous disregard for the rights of third  
11 parties. *CDT I*, 513 F.3d 1085. Despite these determinations, the Ninth Circuit initially upheld  
12 the seizures. The dissent strenuously argued the decision was unfounded, ignored factual  
13 findings of the lower courts, and would have dire ramifications. As Judge Thomas stated,  
14 "Today's decision marks the return of the prohibited general warrant through an endorsement of  
15 a disguised impermissible general search warrant—a tactic we rejected in *United States v. Rettig*,  
16 589 F.2d 418 (9th Cir. 1978)." *Id.* at 1143 (Thomas, J., concurring in part, dissenting in part).

17 The case was then taken *en banc*. *CDT II*, 579 F.3d 989. The *en banc* panel reversed and  
18 ordered the return of all testing results, save the ten athletes named in the first warrant. The  
19 majority explored the government's improper conduct and further reflected on the balance  
20 between law enforcement's perhaps legitimate need to over-seize in conducting searches of ESI  
21 devices, with the Fourth Amendment's prohibition on general or overbroad searches. To strike  
22 this balance, the court directed magistrate judges to adhere to the following five guidelines:

---

23 <sup>8</sup> One judge allowed the government to retain the materials regarding the ten players identified in  
the initial warrant. The subpoenas at issue were also quashed.

- 1 1. Magistrate[ ] [Judges] should insist that the government waive  
2 reliance upon the plain view doctrine in digital evidence cases.
- 3 2. Segregation and redaction must be either done by specialized  
4 personnel or an independent third party. If segregation is to be  
5 done by government computer personnel, it must agree in the  
6 warrant application that the computer personnel will not disclose to  
7 the investigators any information other than that which is the target  
8 of the warrant.
- 9 3. Warrants and subpoenas must disclose the actual risks of  
10 destruction of information as well as prior efforts to seize that  
11 information in other judicial fora.
- 12 4. The government's search protocol must be designed to uncover  
13 only the information for which it has probable cause, and only that  
14 information may be examined by the case agents.
- 15 5. The government must destroy or, if the recipient may lawfully  
16 possess it, return non-responsive data, keeping the issuing  
17 magistrate informed about when it has done so and what it has  
18 kept.

19 *Id.* at 1006.

20 On September 13, 2010, the Ninth Circuit issued a revised *en banc* opinion. *CDT III*, 621  
21 F.3d 1162. The new opinion did not change the outcome of the first *en banc* decision, but the  
22 five guidelines that were previously part of the majority decision became part of a concurring  
23 opinion authored by Chief Judge Kozinski. In his concurrence, joined by four other judges,  
Chief Judge Kosinski notes the guidelines are “hardly revolutionary,” are “essentially *Tamura’s*  
solution to the problem of necessary over-seizing of evidence,” and also offer “the government a  
safe harbor, while protecting the people's right to privacy and property in their papers and  
effects.” *Id.* at 1178, 1180 (Kozinski, C.J., concurring).

In the Court’s view, the Ninth Circuit’s final *en banc* opinion does not permit the  
issuance of the warrant the government seeks in this case for four reasons. First, although the  
five guidelines are no longer mandatory, the majority did not hold magistrate judges are

1 prohibited from employing them or that they are improper or inappropriate. Rather the Court,  
2 exercising its independent judgment, as it must, has arrived at the conclusion that some of the  
3 guidelines should be applied based on the specifics of the present case.<sup>9</sup> *See id.* at 1178  
4 (Kozinski, C.J., concurring). It is also important to note that the Court does not and will not  
5 robotically apply the five guidelines. For example, the Court is satisfied, in this particular case,  
6 that the fifth guideline's concern is met by the government's representations that it will return the  
7 devices unless they are found to be instrumentalities of the criminal offenses named in the  
8 warrant.

9 Second, the warrant application in *CDT III* was drafted in a manner designed to ensure  
10 that it would be lawful and comport with the requirements of the Fourth Amendment. The  
11 warrant contained a panoply of safeguards absent here. As the Ninth Circuit stated "the  
12 magistrate judge . . . wisely made such broad seizure subject to certain procedural safeguards."  
13 *CDT III*, 621 F.3d at 1168. Germane to the present case, these safeguards included: (1) that  
14 investigative agents not review and segregate the data; (2) that specialized forensic computer  
15 search personnel review and segregate the data and not give it to the investigative agents; and (3)  
16 seized evidence outside the scope of the warrant be returned within 60 days.

---

17  
18 <sup>9</sup> Parenthetically, the Court notes the distinction between searching a "third party" computer, as  
19 was the case in *CDT III*, and searching a suspect's computer, would be a distinction without a difference.  
20 First, the Ninth Circuit stated *CDT III* was "more generally . . . about the procedures and safeguards that  
21 federal courts must observe in issuing and administering search warrants and subpoenas for electronically  
22 stored information," not about searches of a third party computer. *CDT III*, 621 F.3d at 1165-66. Second,  
23 in rejecting the government's argument that it could seize items in "plain view," the Court gave several  
examples including: "Can't find the computer? Seize the Zip disks under the bed in the room where the  
computer once might have been." *Id.* at 1171. In giving this example, the Court cited to *United States v.*  
*Hill*, 322 F.Supp.2d 1081 (C.D. Cal 2004), a case involving the search of an individual's computer and  
residence. *Id.* And third, in *CDT III*'s "concluding thoughts" section, the Ninth Circuit stated that a  
broad computer search "calls for greater vigilance on the part of judicial officers in striking the right  
balance between the government's interest in law enforcement and the *right of individuals* to be free from  
unreasonable searches and seizures." *Id.* at 1177 (emphasis added).

1 The *CDT III* court endorsed these safeguards noting that the government's argument the  
2 investigative agents could access all data seized is nothing but "sophistry." *Id.* at 1172. As the  
3 Court stated, "it would make no sense to represent that computer personnel would be used to  
4 segregate data if investigative personnel were also going to access all the data seized. What  
5 would be the point?" *Id.* The court found the government's failure to follow this procedural  
6 protection to reach information not covered by the warrant was a "callous disregard of the Fourth  
7 Amendment," not only because of the binding findings of the district court, but also as matter of  
8 "simple common sense." *Id.*

9 Hence, there is nothing in *CDT III* indicating it is unwise for a magistrate judge to require  
10 the warrant application contain such safeguards where requests for broad computer searches are  
11 made, that such safeguards are inappropriate, or that once such safeguards are ordered, it is  
12 permissible for the government to ignore them. These safeguards are particularly appropriate in  
13 this case. According to the affidavit, the target of the search is a disabled man who conducts  
14 business out of his home. There is no evidence he is using the computer to create illegal copies,  
15 but the computer is likely to store information regarding his supplier, customers and financial  
16 transactions. There is no suggestion that utilizing a filter team in this investigation would  
17 compromise the government's ability to prosecute this case. There is no suggestion that  
18 requiring waiver of the plain view doctrine as a *quid pro quo* for the evident over-seizing will  
19 compromise the government's ability to prosecute this case.

20 In contrast to the warrants issued in *CDT III*, the government, here, applies for the  
21 broadest warrant possible - the authority to search every single thing - but minus any of the  
22 procedural safeguards the Ninth Circuit in *CDT III* deemed to be wise. Perhaps the government  
23 believes that its promise to use "only those methodologies, techniques and protocols as may



1 reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be  
2 seized” is a sufficient safeguard. *Larson Aff.* ¶ 46(d). However, such protection is illusory and  
3 does not justify the government’s request to conduct a search without a filter team and to rely on  
4 the plain view doctrine. Once the Court authorizes the government to search all data, the  
5 government can, and will.

6 Third, the *CDT III* opinion rejected the government’s arguments that under *United States*  
7 *v. Tamura*, 694 F.2d 591 (9th Cir. 1982), it did not have to return any data it found about  
8 baseball players outside the scope of the first warrant because that evidence was in “plain view”  
9 when agents examined the Tracey Directory. Calling this argument “too clever by half” the  
10 Ninth Circuit found the “point of the *Tamura* procedures is to maintain the privacy of materials  
11 that are intermingled with seizable materials, and to avoid turning a limited search . . . into a  
12 general search . . . .” *CDT III*, 621 F.3d at 1170. The government’s claim that everything is in  
13 “plain view” when it is given permission to search broadly would “make a mockery of *Tamura*  
14 and render the carefully crafted safeguards in the Central District warrant a nullity.” *Id.* at 1171.  
15 Hence, while the *CDT III* majority opinion does not state the government in all cases “must  
16 foreswear reliance on the plain view doctrine,” the opinion essentially requires as much.<sup>10</sup>

17 The instant warrant application goes a step beyond the position it took in *CDT III*. In this  
18 case, not only does the government fail to foreswear reliance on the plain view doctrine, it  
19 requests that it be allowed to seek a warrant that permits it to obtain a second warrant to seize  
20

---

21 <sup>10</sup> The Court notes a generalized seizure of ESI would be justified where there is probable cause  
22 to conclude that the entirety of the contents of the ESI device is evidence of crime. *Cf. United States v.*  
23 *Kow*, 58 F.3d 423, 427 (9th Cir. 1995) (“A generalized seizure of business documents may be justified if  
the government establishes probable cause to believe the entire business is merely a scheme to defraud or  
that all of the business’s records are likely to evidence criminal activity.”). Here, the government has not  
presented any evidence that in this case, Mr. Krause’s ESI devices contain only evidence of criminal  
activity.

1 additional evidence whether it was found in the initial search in plain view or not.

2 And fourth, the Ninth Circuit's "concluding thoughts" in *CDT III* put to rest any notion  
3 the warrant sought here is appropriate. Broad searches of ESI devices create "a serious risk that  
4 every warrant for electronic information will become, in effect, a general warrant, rendering the  
5 Fourth Amendment irrelevant." *Id.* at 1176. The Ninth Circuit further provided:

6 Once a file is examined . . . the government may claim (as it  
7 did in this case) that its contents are in plain view and, if  
8 incriminating, the government can keep it. Authorization to search  
9 some computer files therefore automatically becomes authorization  
to search all files in the same sub-directory, and all files in an  
enveloping directory, a neighboring hard drive, a nearby computer  
or nearby storage media.

10 . . .

11 . . . It is not surprising, then, that all three of the district judges  
below were severely troubled by the government's conduct in this  
12 case. Judge Thomas, too, in his panel dissent, expressed  
frustration with the government's conduct and position, calling it a  
"breathtaking expansion of the 'plain view' doctrine, which clearly  
has no application to intermingled private electronic data.

13 . . .

14 We recognize the reality that over-seizing is an inherent part of  
the electronic search process and proceed on the assumption that,  
15 when it comes to the seizure of electronic records, this will be far  
more common than in the days of paper records. This calls for  
greater vigilance on the part of judicial officers in striking the right  
16 balance between the government's interest in law enforcement and  
the right of individuals to be free from unreasonable searches and  
17 seizures. The process of segregating electronic data that is seizable  
from that which is not must not become a vehicle for the  
18 government to gain access to data which it has no probable cause  
to collect.

19 *Id.* at 1176-77.

20 In this case, the Court finds that the requested warrant application impermissibly grants  
21 the government a general or overbroad search warrant in violation of the Constitution and the  
22 law of the Circuit. The Court also reaches this conclusion while recognizing that quite often,  
23 broad searches of digital devices and "over-seizing is an inherent part of the electronic search

1 process.”<sup>11</sup> However, a balance must be struck between the government’s investigatory interests  
2 and the right of individuals to be free from unreasonable searches and seizures. Few computers  
3 are dedicated to a single purpose; rather, computers can perform many functions, such as “postal  
4 services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping  
5 malls, personal secretaries, virtual diaries, and more.” *United States v. Andrus*, 483 F.3d 711,  
6 718 (10th Cir. 2007) (citing Orin S. Kerr, *Searches and Seizures in the Digital World*, 119 Harv.  
7 L. Rev. 531, 569 (2005)). Almost every hard drive encountered by law enforcement will contain  
8 records that have nothing to do with the investigation. To maintain the balance between the  
9 government’s investigatory interests and the Fourth Amendment, the Court is ready to grant the  
10 government’s instant application on the conditions set forth in this opinion. But the government,  
11 much like it did in the *CDT* line of cases, does not seek to perform the search with constitutional  
12 safeguards, i.e., a filter team or foreswearing reliance on the plain view doctrine. The  
13 government’s warrant application therefore does not pass Constitutional muster, and cannot be  
14 squared with the Ninth Circuit’s opinion in *CDT III*.

15 E. *The Fourth Amendment and Use of “Hash Values”*

16 The instant warrant search protocol also purports to authorize the government to use hash  
17 values to perform the search. The government’s proposed use of hash values does not  
18 necessarily narrow the scope of the search requested. Specifically, although “hash values” can  
19 be used to exclude files that do not interest the government such as a digital device’s operating  
20 system, they can also be used to search and find evidence outside the scope of the warrant  
21 automatically and systematically. This is because most law-enforcement forensic software can  
22 automatically search for evidence of other crimes, such as child pornography, based on known

23 \_\_\_\_\_  
<sup>11</sup> *CDT III*, 621 F.3d at 1177.

1 hash values. *See United States v. Mann*, 592 F.3d 779, 783-84 (7th Cir. 2010) (detective ignored  
2 warrant limitations and conducted general search using Forensic Tool Kit (FTK) and its  
3 accompanying “KFF alert system” to locate child pornography).

4 The instant warrant application proposes to use “hash values,” but contained no  
5 restrictions on that use, allowing the government to search for evidence of crime for which is  
6 lacks probable cause, such as child pornography. Moreover, the warrant affidavit does not  
7 demonstrate “hash values” exist that can be used to ferret out the evidence for which the  
8 government has probable cause in this case. The Court concludes that the following language  
9 must be added to the instant warrant application in order to address the problems with using hash  
10 values:

11 However, these methodologies, techniques and protocols will not  
12 include the use of “hash value” libraries to search the electronically  
13 stored information for items that are not set forth in the items  
authorized to be seized in Attachment B of this warrant.

14 As this new language is necessary to address both the scope and reasonableness of the search the  
15 conduct seeks to conduct, it must be included in the government’s ESI application.

### 16 III. CONCLUSION

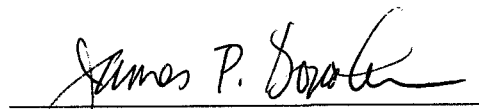
17 This Court is required under the U.S. Constitution and the law of the Circuit to deny the  
18 instant warrant application. Counterfeiting products is a serious crime and costs American  
19 intellectual property owners billions of dollars annually, results in lost jobs, and creates  
20 substantial threats to consumers of these products. Probable cause exists to search Mr. Cunnius’  
21 digital devices for evidence relating to counterfeit products. But the government asks the Court  
22 to do what the law does not permit. The government would have the Court give it the authority  
23 to scour all data contained in the seized digital devices, and more, without any of the procedural  
protections *CDT III* deemed both wise and necessary, and the authority to obtain a second

1 warrant to seize any other data found outside the scope of the first warrant whether it was found  
2 in plain view or not. This request is exactly what *CDT III* prohibited: "the process of segregating  
3 electronic data that is seizable from that which is not must not become a vehicle for the  
4 government to gain access to data which it has no probable cause to collect." *Id.* at 1177.  
5 Moreover, if the Court sanctions this action, its decision effectively becomes non-reviewable.  
6 *See United States v. Leon*, 468 U.S. 897 (1984).

7 *CDT III* provided strong guidance to this Court regarding ESI searches. While the  
8 guidelines are not mandatory, most are appropriately required in this case. The government may  
9 disagree with the decision enunciated in *CDT III*. The government's options, however, are to  
10 seek review of *CDT III* with the U.S. Supreme Court or to comply. Neither the government nor  
11 this Court has the option to pretend that *CDT III* does not exist. Because the Court finds the  
12 government's warrant application, without the protections set forth in this Order, fails to comply  
13 with the Fourth Amendment and the law of this Circuit, the Court DENIES the government's  
14 application for a search warrant.

15 As this matter involves an on-going criminal investigation, the Clerk of Court is directed  
16 to file this Order under seal. This Order will be unsealed at the earlier of when any warrant  
17 relating to this matter is executed, or when a decision is made not to proceed with the  
18 prosecution of the matter, or otherwise by written order. A copy of this Order shall also be  
19 provided to the United States and the assigned United States District Judge.

20 DATED this 11th day of February, 2011.

21   
22 JAMES P. DONOHUE  
23 United States Magistrate Judge

# Exhibit

# 1



# UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

The residence located at 2305 Rucker Avenue,  
Apt. 5, Everett, Washington 98201

Case No.

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is incorporated herein by reference

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18 U.S.C. § 2319  
18 U.S.C. § 2320

Offense Description  
Criminal Copyright Infringement  
Trafficking in Counterfeit Goods

The application is based on these facts:

See attached Affidavit of Special Agent Michael J. Larson, attached hereto and incorporated herein.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of        days (give exact ending date if more than 30 days:                     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA MICHAEL J. LARSON, Affiant

Printed name and title

Sworn to before me and signed in my presence.

Date:                     

Judge's signature

City and state: Seattle, Washington

JAMES P. DONOHUE, U.S. Magistrate Judge

Printed name and title

## **ATTACHMENT A**

### **SUBJECT PREMISES**

The SUBJECT PREMISES at 2305 Rucker Avenue, Apartment 5, Everett, Washington 98201 is more fully described as:

a two-story apartment building located near the intersection of Rucker Avenue and 23rd Street. The apartment building is tan or taupe in color; however, the lower level of the west side of the structure has a red brick facade. The west side of the house has a red entry door, and a single-car garage door. The number two thousand three hundred five (2305) is affixed to the brick facade to the left of the red entry door. On the north side of the building, there is a covered external stairway with entry doors on both the upper and lower levels. Apartment number five is located on the upper level of the building and the entry door to the unit is light green in color and marked with the number five.

## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

The items to be seized are the following items that constitute evidence, fruits, and instrumentalities of the crimes of Criminal Copyright Infringement in violation of Title 18, United States Code, Section 2319 and Trafficking in Counterfeit Goods in violation of Title 18, United States Code, Section 2320.

1. The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, digital and magnetic form (in storage on or in media such as tapes, cassettes, hard disks, floppy disks, diskettes, compact disks, CD-ROMs, DVDs, optical disks, printer buffers, smartcards, electronic notebooks, memory cards, USB thumb drives, mobile or cellular phones, personal data assistants, or any other storage medium):

a. Counterfeit software and counterfeit software components including, boxes, labels, packaging, stickers, wrappers, emblems, medallions, documentation, license agreements, manuals, end user license agreements, and/or certificates of authenticity;

b. Records relating to the purchase and/or sale of software including invoices, purchase orders, correspondence with customers and/or suppliers of software, inventory lists, advertisements;

c. Records relating to the exporting or importing of computer software to or from countries other than the United States;

d. Records relating to licensing agreements for the distribution of computer software;

e. Shipping records including U.S. Mail, Federal Express, United Parcel Service, or any other common carrier;

f. Correspondence with Customs and Border Protection regarding any seizures of counterfeit software;

g. Correspondence with Microsoft Corporation or its affiliates regarding the distribution of counterfeit software;

h. Any books, papers, internet history, documents, pamphlets, or other

materials regarding counterfeit software;

i. Records related to the posting of advertisements for the sale of software on Internet classified advertising services such as eBid, Craigslist, Amazon.com and/or eBay, including drafts of advertisements, photographs of products advertised, account information, sales history, customer feedback reports, payment records, customer complaints, and correspondence with the classified advertisement service provider;

j. Any and all financial records present at the subject premises, including: checking and savings account bank statements; deposit or withdrawal records; safe deposit box records and keys; investment or brokerage account statements; cashier's check receipts; check books; receipts; wire transfer records; electronic funds transfer records; cancelled checks; credit card account statements and receipts; records of employment and earnings; bank loan or credit applications; business books and records; and telephone records;

k. Any and all evidence of dominion and control of the subject premises and/or any digital devices located at the subject premises;

l. Any and all United States currency, cashier's checks, money orders, travelers checks, and other monetary instruments;

2. Digital devices and/or their components, including:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data related to criminal copyright infringement and/or trafficking in counterfeit goods, including modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

e. Any physical keys, encryption devices, dongles and similar physical

items that are necessary to gain access to the computer equipment, storage devices or data; and

f. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

g. Evidence of who used, owned or controlled any seized digital device/s at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

h. Evidence of the attachment to the digital device/s of other storage devices or similar containers for electronic evidence;

i. Evidence of counter-forensics programs (and associated data) that are designed to eliminate data from a digital device;

j. Evidence of the times the digital device/s was used.

k. Any other ESI from the digital device/s necessary to understand how the digital device was used, the purpose for its use, who used it, and when.

**AFFIDAVIT**

STATE OF WASHINGTON  
COUNTY OF KING

SS

I, Michael J. Larson, being first duly sworn, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Department of Homeland Security, United States Immigration and Customs Enforcement (ICE), assigned to the Office of the Special Agent in Charge, Seattle, Washington, and have been so employed since July of 2009. During my tenure with ICE, I have been assigned to the Border Enforcement Security Task Force (BEST) and have participated in investigations and search warrants involving theft, fraud, smuggling, counterfeit goods, and drug trafficking. Prior to my employment with ICE, I worked for the United States District Court for the Western District of Washington for eleven years as a United States Probation Officer and United States Probation Officer Assistant. I am a graduate of the Federal Law Enforcement Training Center's Criminal Investigator Training Program in Brunswick, Georgia, as well as the ICE Special Agent Training Program. I am also a graduate of Michigan State University in East Lansing, Michigan, where I received Bachelors degrees in International Relations and Criminal Justice from James Madison College and the School of Criminal Justice, respectively.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 2305 Rucker Avenue, Apartment 5, Everett, Washington, 98201, hereinafter "SUBJECT PREMISES," as more fully described in Attachment A to this Affidavit, for the property and items described in Attachment B to this Affidavit.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records



1 related to this investigation; communications with others who have personal knowledge  
2 of the events and circumstances described herein; and information gained through my  
3 training and experience.

4 4. Because this Affidavit is submitted for the limited purpose of establishing  
5 probable cause in support of the application for a search warrant, it does not set forth each  
6 and every fact that I or others have learned during the course of this investigation. I have  
7 set forth only the facts that I believe are necessary to establish probable cause to believe  
8 that evidence, fruits and instrumentalities of violations of Title 18, United States Code,  
9 Sections 2319 (Criminal Copyright Infringement ) and 2320 (Trafficking in Counterfeit  
10 Goods) will be found at the SUBJECT PREMISES and on any digital devices located at  
11 the SUBJECT PREMISES.

#### 12 SUMMARY OF INVESTIGATION

13 5. In October 2010, I received information from Microsoft Corporation  
14 regarding an individual they believed was selling counterfeit Microsoft software via the  
15 internet classified advertising service Craigslist. According to Microsoft investigator  
16 Steve Studhalter, EDWARD CUNNIUS was responsible for numerous Craigslist  
17 advertisements over the past few months that offered to sell brand new, in the box,  
18 Microsoft software at prices well below typical retail prices for the same software. In  
19 addition, Mr. Studhalter informed me that a shipment of counterfeit Microsoft software  
20 from China, addressed to EDWARD CUNNIUS, had been seized by Customs and Border  
21 Protection (CBP) on October 18, 2010. Following the October 18, 2010 CBP seizure,  
22 Microsoft sent Mr. CUNNIUS a letter warning him of the consequences of distributing  
23 counterfeit software and informing him how he might detect counterfeit software to  
24 ensure he does not engage in further distribution of counterfeit software. Microsoft  
25 subsequently initiated an undercover test purchase of software from Mr. CUNNIUS at his  
26 home in Everett, Washington and purchased several products at prices substantially below  
27 retail value. An examination of the software products purchased from Mr. CUNNIUS  
28 revealed the products were counterfeit.

1           6.     I later initiated two law enforcement undercover test purchases from Mr.  
2 CUNNIUS at his residence in Everett, Washington. On each occasion, agents with ICE  
3 contacted Mr. CUNNIUS in response to Craigslist advertisements offering the sale of  
4 Microsoft software at prices well below retail. Agents met Mr. CUNNIUS at his  
5 apartment in Everett, Washington on December 13, and December 21, 2010, and  
6 purchased several boxes of purportedly genuine, new, in the box, Microsoft software.  
7 During each undercover purchase, Mr. CUNNIUS retrieved the software packages from a  
8 closet in the bedroom of his apartment. Mr. CUNNIUS was evasive in response to  
9 questions about the authenticity of the product and stated that if customers complained, he  
10 would instruct them to go buy the products for much higher prices at retail  
11 establishments. All of the products purchased from Mr. CUNNIUS by the undercover  
12 agents were submitted to Microsoft for analysis by their product identification specialists  
13 who determined that each of the products were counterfeit.

#### 14                                   THE INVESTIGATION

15           7.     On October 27, 2010, I spoke to Microsoft anti-piracy investigator Steve  
16 Studhalter who told me about a suspect who recently had a shipment of counterfeit  
17 Microsoft software seized by Customs and Border Protection. According to Mr.  
18 Studhalter, on October 18, 2010, CBP had seized an inbound shipment of counterfeit  
19 Microsoft software from China, addressed to EDWARD RUSSELL CUNNIUS at 2305  
20 Rucker Avenue #5, Everett, Washington. Mr. Studhalter also told me that this suspect  
21 had been advertising Microsoft software on Craigslist at suspiciously low prices on a  
22 regular basis over the past several months. I know based on my training and experience  
23 in conducting investigations of counterfeit products and from information I have received  
24 from Microsoft anti-piracy investigators, that one indication of potentially counterfeit  
25 product is the price at which the product is sold. Products sold for prices far below the  
26 typical retail price are often found to be counterfeit. Mr. Studhalter e-mailed screen clips  
27 of several recent Craigslist advertisements by Mr. CUNNIUS that offered to sell products  
28

1 such as Microsoft Office Professional 2010 and Microsoft Visio Professional 2010 at  
2 prices up 75% off retail value.

3 8. According to Mr. Studhalter, in response to the CBP seizure, Microsoft had  
4 sent a warning letter to Mr. CUNNIUS at his Everett home on October 22, 2010. The  
5 letter advised Mr. CUNNIUS that it had received information that Mr. CUNNIUS or  
6 someone with his company may have distributed illegal and/or unlicensed Microsoft  
7 software and informed Mr. CUNNIUS of the consequences of illegal distribution. The  
8 letter also notified Mr. CUNNIUS of the various types of software piracy including  
9 counterfeit software distribution. Finally, the letter advised Mr. CUNNIUS how to  
10 protect his business by obtaining legitimate Microsoft software from authorized retail  
11 distributors and by learning how to differentiate genuine Microsoft software from  
12 counterfeit and infringing software.

13 9. Mr. Studhalter also told me that he planed to initiate a "test purchase" from  
14 Mr. CUNNIUS. A test purchase is an undercover operation in which a private  
15 investigator employed by Microsoft purchases software from a suspected counterfeit  
16 software distributor. Test purchases may be initiated via telephone, over the internet, or  
17 in person depending on how the particular suspect conducts business. Product purchased  
18 during a test purchase is later examined by Microsoft product identification specialists in  
19 order to determine whether the product is genuine or counterfeit.

20 10. After speaking to Mr. Studhalter on October 27, 2010, I retrieved a copy of  
21 a CBP incident report from the Treasury Enforcement Communications System (TECS).  
22 The report, dated October 18, 2010, indicated that CBP-San Francisco seized, 10 pieces  
23 of Windows Ultimate software on October 18, 2010, at the San Francisco international  
24 mail station. CBP reported the shipment was valued at \$1,350.00 and was sent via Air  
25 Express parcel from China, addressed to "Edward Cunnius" at 2305 Rucker Avenue #5,  
26 Everett, WA 98201 (the SUBJECT PREMISES). According to the report, the software  
27 inside the parcel was determined to be counterfeit based on the fact that clear labels were  
28 adhered to the surface of the disks, whereas a genuine Microsoft product does not have

1 this feature. In addition, when the labels were lifted up, the portions of the hologram on  
2 the disc came up with the label. A genuine Microsoft disk has the hologram embedded in  
3 the disk and, therefore, the hologram would not come up with the label. Following the  
4 seizure, CBP sent a notice of seizure to Mr. CUNNIUS addressed to "2305 Rocker [sic]  
5 Ave. #5, Everett, Washington 98201." The notice informed Mr. CUNNIUS that the  
6 software was counterfeit and violated a trademark registered by the Microsoft  
7 Corporation. The notice further informed Mr. CUNNIUS that the software was subject to  
8 forfeiture.

9 11. I reviewed records from the Washington State Department of Licensing that  
10 indicate EDWARD RUSSELL CUNNIUS and Judith Ann CUNNIUS are the only  
11 registered drivers at 2305 Rucker Avenue #5, Everett, Washington 98201. I also obtained  
12 a copy of Mr. and Ms. CUNNIUS' driver's license photographs.

13 12. I have reviewed a report prepared by Randy Mullinax of R.E. Mullinax  
14 Investigations, LLC that indicates Mr. Mullinax conducted a test purchase from Mr.  
15 CUNNIUS on October 28, 2010. According to Mr. Mullinax, he contacted Mr.  
16 CUNNIUS on October 27, 2010, at a telephone number listed in a Craigslist  
17 advertisement for the sale of Microsoft Office Professional 2010. The man who  
18 answered the telephone identified himself as "Ed" and stated that he had two copies of  
19 Office Professional 2010 left. Mr. Mullinax reported that "Ed" told him to come to his  
20 apartment at 2305 Rucker Street, #5, Everett, Washington the following day to purchase  
21 the software. On October 28, 2010, Mr. Mullinax drove to the SUBJECT PREMISES  
22 and met with Mr. CUNNIUS. Mr. CUNNIUS sold Mr. Mullinax one copy each of  
23 Microsoft Windows 7 Ultimate, Microsoft Visio Professional 2010, and Microsoft Office  
24 Professional 2010. The total price for all three products was \$350.00. According to Mr.  
25 Studhalter, the estimated retail price of these three products combined is \$1,377.00. Mr.  
26 Mullinax reported that Mr. CUNNIUS stated that the product was "not counterfeit" and  
27 he claimed he obtained the software from someone he knew who bought it from  
28 Microsoft in Redmond, Washington. However, Mr. CUNNIUS also stated that if there

1 was a problem with the software registering correctly, Microsoft might tell Mr. Mullinax  
2 that the software is counterfeit.

3 13. I have reviewed three sample analysis reports prepared by Microsoft  
4 product identification specialist Lisa Blinzler. Ms. Blinzler examined each of the  
5 products purchased by Mr. Mullinax on October 28, 2010, and determined that all three  
6 products were counterfeit. She reported that each of the items contained counterfeit  
7 certificates of authenticity labels, ultra-violet ink was missing from the product key  
8 labels, and there were typographical errors on the product boxes among other indications  
9 that the product and packaging were counterfeit.

10 14. On December 13, 2010, at approximately 9:40 a.m., Special Agent Shawn  
11 Galetti, initiated telephonic contact with Mr. CUNNIUS for the purpose of purchasing the  
12 following Microsoft software: Visio Professional 2010 and Project Professional 2010. In  
13 the days and weeks leading up to this contact, Mr. CUNNIUS frequently advertised  
14 Microsoft software on Craigslist and directed interested parties to contact him at  
15 425-339-2555. Agent Galetti contacted Mr. CUNNIUS at this telephone number. During  
16 the contact, Mr. CUNNIUS identified himself as "Ed" and stated that he could meet with  
17 Agent Galetti anytime before 6:00 p.m. Mr. CUNNIUS refused Agent Galetti's request  
18 to meet at neutral site stating that he was on disability and did not drive. Mr. CUNNIUS  
19 said his address was 2305 Rucker Avenue, Apartment 5, Everett, Washington 98201, and  
20 arranged to meet with Agent Galetti between 12:30 p.m. and 1:30 p.m. Agent Galetti's  
21 conversation with Mr. CUNNIUS was audio recorded, and I was present during the  
22 contact.

23 15. At approximately 12:42 p.m. on December 13, 2010, Agent Galetti and  
24 Agent Marcus Browne, acting in an undercover capacity, contacted Mr. CUNNIUS at the  
25 SUBJECT PREMISES. During their contact with Mr. CUNNIUS, one of the agents was  
26 wired for video and audio with an undercover recording device. The entire contact was  
27 taped and I have reviewed the tape. Shortly after the agents arrived, Mr. CUNNIUS went  
28 to a back room of his apartment and returned a short time later with one copy of



1 Microsoft Visio Professional 2010 and one copy of Microsoft Project Professional 2010.  
2 Agent Galetti asked Mr. CUNNIUS if there were any problems with the software. Mr.  
3 CUNNIUS advised Agent Galetti to remove any "trial versions" from his computer  
4 before running the new software. Mr. CUNNIUS also stated that he had received the  
5 software about four months ago and that it cost as much as "a thousand dollars a piece" at  
6 Best Buy. He claimed he bought the product from a "third party." When Agent Galetti  
7 asked if Mr. CUNNIUS had received any complaints related to the software, Mr.  
8 CUNNIUS assured Agent Galetti that he had not received any customer complaints.  
9 Agent Galetti paid Mr. CUNNIUS with \$225.00 in U.S. currency for the software and  
10 asked whether Mr. CUNNIUS had any other software for sale. Mr. CUNNIUS responded  
11 that he also had copies of Windows 7 Ultimate for \$125.00, and Office Professional 2010  
12 for \$100.00.

13 16. While speaking to Agents Galetti and Browne, Mr. CUNNIUS received a  
14 telephone call from an unknown individual. Based on Mr. CUNNIUS' responses to the  
15 caller and his comments to Agents Galetti and Browne immediately after the call, it  
16 appeared the caller had questioned the authenticity of the software in the Craigslist  
17 posting. Mr. CUNNIUS advised the caller he "got it from a third party," and "they are  
18 not from the Microsoft store" and that it did not "say 'not for resale' on em" Immediately  
19 after the call, Mr. CUNNIUS advised Agents Galetti and Browne that there were some  
20 people who wanted to "look a gift horse in-the-mouth" or they "just ain't happy what they  
21 see" and "they want to make a big deal about it." Mr. CUNNIUS said he would direct  
22 those people to the "door" and tell them "Best Buy is down the street about three miles -  
23 make sure you have a deep pocket."

24 17. On December 14, 2010, I provided the boxes of software that Agents  
25 Galetti and Browne purchased from Mr. CUNNIUS to Microsoft product identification  
26 specialist Brittany Carmichael who inspected the software and determined it was  
27 counterfeit. Ms. Carmichael completed a sample analysis report for each of the two  
28 pieces of software and reported that each of the items contained counterfeit certificates of

1 authenticity labels, the ultra-violet ink was missing from the product key labels, and there  
2 were typographical errors on the product boxes among other indications that the product  
3 and packaging were counterfeit. These were the same counterfeit features discovered  
4 earlier on the counterfeit software that Mr. Mullinax purchased from Mr. CUNNIUS on  
5 October 28, 2010. According to Microsoft the software that Agents Galetti and Browne  
6 purchased for \$225.00 had an estimated retail price of approximately \$1,560.00.

7 18. On December 21, 2010, at approximately 9:40 a.m., Agent Galetti called  
8 Mr. CUNNIUS again and asked about Craigslist advertisements Mr. CUNNIUS had  
9 posted for the sale of Microsoft Office Professional 2010, Windows 7 Home Premium,  
10 Windows 7 Professional, and Windows 7 Ultimate. Mr. CUNNIUS agreed to meet Agent  
11 Galetti during the lunch hour at the SUBJECT PREMISES.

12 19. At approximately 11:45 a.m. on December 21, 2010, Agents Galetti and  
13 Browne, again acting in undercover capacity, contacted Mr. CUNNIUS at the SUBJECT  
14 PREMISES. During their contact with Mr. CUNNIUS, one of the agents was wired for  
15 video and audio with an undercover recording device. The entire contact was taped and I  
16 have reviewed the tape. Agent Galetti told Mr. CUNNIUS that he resold the software he  
17 bought from him on December 13, 2010, and made a good profit. Agent Galetti said  
18 there was demand for additional product and asked if Mr. CUNNIUS could contact his  
19 supplier to see if he or she would work with Agent Galetti. Mr. CUNNIUS said it took  
20 him years to make his contact and that he gets his product through the mail. He told  
21 Agent Galetti that he communicated with his source via electronic mail and paid him  
22 through electronic transfer from his bank. Agent Galetti told Mr. CUNNIUS that he was  
23 interested in making money and asked if Mr. CUNNIUS would introduce him to his  
24 source. Mr. CUNNIUS said he did not believe his source would talk to Agent Galetti.  
25 Mr. CUNNIUS also claimed the product was genuine and he had not experienced any  
26 trouble with the product. However, he said some people said they did not think the  
27 product was "legit" and he would tell them to "go to the store and pay \$500.00."



20. After speaking to Agents Galetti and Browne about his source, Mr. CUNNIUS walked to a back bedroom where he opened a closet and produced the requested software. Agent Galetti accepted the software and again asked Mr. CUNNIUS if he could be introduced to his source. Mr. CUNNIUS advised he would speak to his source. Mr. CUNNIUS provided Agent Galetti with one copy each of Microsoft Office Professional 2010, Windows 7 Home Premium, Windows 7 Professional, and Windows 7 Ultimate. Agent Galetti paid Mr. CUNNIUS a total of \$450.00.

21. On December 22, 2010, I provided the boxes of software that Agents Galetti and Browne purchased from Mr. CUNNIUS on December 21, 2010, to Microsoft product identification specialist Brittany Carmichael. Ms. Carmichael inspected the software and determined it was counterfeit based on many of the same counterfeit features discovered on the products purchased on December 13, 2010, and October 28, 2010. According to Microsoft the software that Agents Galetti and Browne purchased on December 21, 2010, for \$450.00 had an estimated retail price of approximately \$1,320.00.

22. I know based on my conversations with Mr. Studhalter and others at Microsoft Corporation that the word Microsoft is a registered trademark on the principal register of the United States Patent and Trade Office. I also know that the word Microsoft is registered as a trademark for the sale of software (among many other uses for which the word Microsoft is a registered trademark).

## RELEVANT STATUTES

### A. Criminal Copyright Infringement

23. Title 17, United States Code, Sections 506(a) and (b) provide in relevant part:

(a) Criminal infringement.--

(1) In general.--Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed--

(A) for purposes of commercial advantage or private financial gain;  
 (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than \$1,000.

**B. Trafficking in Counterfeit Goods**

24. Title 18, United States Code, Section 2320(a) and (b) provide in relevant part:

(a) Whoever; intentionally traffics or attempts to traffic in goods or services and knowingly uses a counterfeit mark on or in connection with such goods or services, or intentionally traffics or attempts to traffic in labels, patches, stickers, wrappers, badges, emblems, medallions, charms, boxes, containers, cans, cases, hangtags, documentation, or packaging of any type or nature, knowing that a counterfeit mark has been applied thereto, the use of which is likely to cause confusion, to cause mistake, or to deceive, shall, if an individual, be fined not more than \$2,000,000 or imprisoned not more than 10 years, or both.

**BACKGROUND REGARDING COPYRIGHTS**

25. Based on my training and experience, I know the United States Copyright Office is an agency of the United States which promotes the progress of the arts and protection for the works of authors. The United States Copyright Office is also the office of record where claims to copyright are registered and where documents relating to copyright may be recorded when the requirements of the copyright law are met.

26. In general terms, copyright is a form of protection provided by law for original works of authorship, including literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations. "Copyright" literally means the right to copy. The term has come to mean that body of exclusive rights granted by law to authors for protection of their work. The owner of a copyright has the exclusive right to reproduce, distribute, and, in the case of certain

1 works, publicly perform or display the work; to prepare derivative works; in the case of  
2 sound recordings, to perform the work publicly by means of a digital audio transmission;  
3 or to license others to engage in the same acts under specific terms and conditions.  
4 Copyright protection does not extend to any idea, procedure, process, slogan, principle, or  
5 discovery.

## 6 BACKGROUND REGARDING TRADEMARKS

7 27. Based on my training and experience, I know the United States Patent and  
8 Trademark Office (USPTO) is an agency of the United States which promotes the  
9 progress of science and the useful arts by securing for limited times to authors and  
10 inventors the exclusive right to their respective writings and discoveries (Article I,  
11 Section 8 of the United States Constitution). Among USPTO's major functions are the  
12 examination and registration of trademarks and the dissemination of trademark  
13 information. Through the registration of trademarks, USPTO assists businesses in  
14 protecting their investments, promoting goods and services, and safeguarding consumers  
15 against confusion and deception in the marketplace. By disseminating trademark  
16 information, USPTO promotes an understanding of intellectual property protection and  
17 facilitates the development and sharing of new technologies worldwide. Registration of a  
18 producer's trademark on USPTO's principal register gives notice to the world of the  
19 producer's exclusive right to use and to protect that trademark.

20 28. In general terms, a trademark is a word, name, symbol, or device, or any  
21 combination thereof, that is intended to distinguish one producer's goods from those of  
22 other producers and to indicate the source of the goods. Trademark law helps ensure that  
23 a trademark can serve this function of distinguishing a producer's goods, because it  
24 prohibits other producers from using a similar mark in a way that is "likely to cause  
25 confusion" among consumers (i.e. by making consumers wonder which producers created  
26 which products). Trademark law broadly prohibits uses of trademarks, trade names, and  
27 trade dress that are likely to cause confusion about the source of a product or service.  
28

**COPYRIGHTS AND TRADEMARKS RELEVANT TO THIS INVESTIGATION**

29. Based on my training and experience, I know that Microsoft develops, advertises, markets, distributes, and licenses a number of computer software programs. Microsoft's software programs are recorded on certain electronic media, including magnetic diskettes, CD-ROMs, and/or DVD-ROMs, and they are packaged and distributed together with associated proprietary materials such as user guides, user manuals, end-user license agreements (EULAs), Certificates of Authenticity (COA), and other components.

30. Microsoft Certificates of Authenticity are special certificates or labeling components that are distributed with Microsoft software programs in order to help end-users verify whether they have genuine Microsoft software. COAs are manufactured with special security features, such as interwoven threads, holograms, and ultra-violet ink, that make unauthorized duplication difficult.

31. Microsoft distributes unique Product Keys to its licensees. Each Product Key consists of a 25-character alphanumeric code arranged in five groups of five characters each. Product Keys are needed to unlock certain software programs and enable their use. Because media containing Microsoft's copyrighted software is capable of being installed on a potentially unlimited number of computers, Microsoft relies on the unique Product Keys, and in some cases activation features within the software, to prevent or at least restrict the installation and use of its software by unauthorized third parties. Product Keys are printed on, among other things, COAs.

32. COAs accompanying Microsoft software provide licensees of genuine Microsoft software with Product Keys that allow such customers to install and run genuine Microsoft software on their computers.

33. There are various restrictions on the distribution of Microsoft software. For example, certain Microsoft Original Equipment Manufacturer (OEM) and System Builder software is licensed for distribution only with a new personal computer (PC). The sale or

1 other distribution of individual copies of OEM or System Builder Microsoft software, not  
2 as part of the distribution of a new PC, is not authorized by Microsoft.

3 34. Based on my knowledge and experience, I know that Microsoft has  
4 registered a number of copyrights, and trademarks and/or service marks, with the United  
5 States Copyright and United States Patent and Trademark Offices, respectively.  
6 Microsoft has been and still is, the sole owner of all rights, title and interest in, and to, its  
7 copyrights, trademarks, and/or service marks, and has made continuous use of these  
8 copyrights, trademarks, and/or service marks.

9 **COMPUTER SEARCH RELATED DEFINITIONS**

10 35. A "forensic image" is a complete and accurate copy of every bit and byte on  
11 the subject drive including hidden, deleted, or encrypted data. A forensic image will  
12 include all data, not just the data available and visible to the user utilizing the devices'  
13 operating system. Law enforcement typically attempts to create a forensic image of any  
14 digital device that may contain data or items within the scope of a search warrant in order  
15 to secure the data in a forensically sound manner prior to conducting a search. Because  
16 data on a digital device is affected by every action of the user, law enforcement will  
17 typically search the forensic image rather than the actual device in order to ensure the  
18 integrity of the data or items searched. The creation of a forensic image of the data to be  
19 searched is analogous to the process of securing a physical search location. A forensic  
20 image may be created of either a physical drive or a logical drive. A physical drive is the  
21 actual physical hard drive that may be found in a typical computer. When law  
22 enforcement creates a forensic image of a physical drive, the image will contain every bit  
23 and byte on the physical drive. A logical drive, also known as a partition, is a dedicated  
24 area on a physical drive that may have a drive letter assigned (for example the c: and d:  
25 drives on a computer that actually contains only one physical hard drive). Therefore,  
26 creating an image of a logical drive does not include every bit and byte on the physical  
27 drive.  
28



1       36. "Email" or electronic mail is a method of exchanging digital messages,  
2 which are transmitted over a communications network, such as the Internet, an internal  
3 network (ie. Local Area Network), or mobile/cellular telephone service.

4                   **PROBABLE CAUSE THAT EVIDENCE WILL BE FOUND**  
5                   **ON DIGITAL DEVICES AT THE SUBJECT PREMISES**

6       37. As set forth above and in Attachment B to this Affidavit, I seek permission  
7 to search for and seize evidence, fruits and instrumentalities of the above-referenced  
8 crimes that might be found on the SUBJECT PREMISES, in whatever form they are  
9 found. Based on the information I have learned in this investigation, I believe evidence  
10 related to how Mr. CUNNIUS obtained counterfeit software, how Mr. CUNNIUS paid  
11 for counterfeit software and how Mr. CUNNIUS distributed counterfeit software is likely  
12 to be discovered on digital devices.<sup>1</sup> Therefore, I am requesting permission to search for  
13 and seize any computers or digital devices that may be located at the subject premises.

14       38. As outlined above, Mr. CUNNIUS stated that he communicates with his  
15 source of software via electronic mail. In addition, Mr. CUNNIUS stated that he paid his  
16 source through electronic transfers from his bank. Furthermore, Agents Galetti and  
17 Browne observed personal computers in Mr. CUNNIUS' apartment and Mr. CUNNIUS  
18 discussed computers extensively with the agents. I also know based on the information  
19 set forth above, that Mr. CUNNIUS advertises the sale of software via the internet  
20 classified service Craigslist and that many of his advertisements contain digital  
21 photographs of the products he advertises for sale. Therefore, I believe digital devices are  
22 likely to be found at the subject premises and that they are likely to contain evidence  
23 including electronic mail correspondence with Mr. CUNNIUS' source, evidence of

24  
25  
26       <sup>1</sup> "Digital device" includes any electronic device capable of processing and/or storing data in  
27 digital form, including, but not limited to: central processing units, laptop or notebook computers,  
28 peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives  
intended for removable media, related communications devices such as modems, cables and connections,  
electronic storage media, electronic/digital security devices, wireless communication devices such as  
telephone paging devices, beepers, mobile or cellular telephones, personal data assistants ("PDAs"),  
iPods, blackberries, digital cameras, and digital gaming devices.

1 internet banking transactions, and evidence of his advertisements and marketing of  
2 counterfeit software.

3 39. I also know based on my training and experience that computers may be  
4 utilized by more than one user. In order to determine exactly who else may be  
5 responsible for obtaining and trafficking in the counterfeit software purchased from Mr.  
6 CUNNIUS, I am asking for permission to search for evidence of dominion and control of  
7 any digital device located at the subject premises. In order to determine who may have  
8 been using the computers at the relevant time, I am asking for permission to search for  
9 things such as: 1) evidence of how the digital devices' logins are maintained; 2) whether  
10 the digital devices' are password protected; 3) whether there are multiple accounts on the  
11 digital devices; 4) what accounts are on the digital devices; 5) internet history that may  
12 reveal the identity of the particular users of the digital devices; 7) evidence of software  
13 that would allow remote access to the computer; 8) evidence of malware or viruses (or the  
14 lack thereof) that would allow others to control the digital devices; 9) evidence of security  
15 software designed to detect and/or defeat malware.

16 **PAST EFFORTS TO OBTAIN EVIDENCE**

17 40. Because of the nature of the evidence that I am attempting to obtain and the  
18 nature of the investigation, I have not made any prior efforts to obtain the evidence based  
19 on the consent of the SUBJECT. Based on my training and experience, I believe that Mr.  
20 CUNNIUS would probably refuse to consent to a search of his residence and any of his  
21 computer equipment and/or digital devices. I also believe, based upon the nature of the  
22 investigation, that if Mr. CUNNIUS becomes aware of the investigation in advance of the  
23 execution of a search warrant, he may attempt to destroy any potential evidence, whether  
24 digital or non-digital, thereby hindering law enforcement agents from the furtherance of  
25 the criminal investigation. Therefore, I have not attempted to obtain this evidence from  
26 Mr. CUNNIUS.

27 41. I am aware of one e-mail account that Mr. CUNNIUS has used in the past.  
28 In January 2011, I interviewed a former customer of Mr. CUNNIUS who stated that Mr.



1 CUNNIUS has an e-mail account with the service provider Comcast. I have not yet  
2 attempted to obtain a search warrant for this account. I may request a search warrant for  
3 this account in the future, depending on the outcome of this search. I believe a search of  
4 Mr. CUNNIUS' computers will yield evidence of his electronic mail communications  
5 with his source and may reveal additional e-mail accounts in addition to the account he  
6 has with Comcast.

#### 7 SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

8 42. Based on my training and experience and my consultation with other agents  
9 who have specialized training and experience in searching for electronic evidence, I know  
10 that every type and kind of information, data, record, sound or image can exist and be  
11 present as electronically stored information on any of a variety of computers, computer  
12 systems, digital devices, and other electronic storage media. I also know that electronic  
13 evidence can be moved easily from one digital device to another. As a result, I believe  
14 that electronic evidence may be stored on any digital device present at the search site.

15 43. Based on my training and experience, and my consultation with other  
16 agents who have specialized training and experience in searching for electronic evidence,  
17 I know that in some cases the items set forth in Attachment B may take the form of files,  
18 documents, and other data that is user-generated and found on a digital device. In other  
19 cases, these items may take the form of other types data – including in some cases data  
20 generated automatically by the devices themselves.

21 44. Based on my training and experience, and my consultation with other agents  
22 who have specialized training and experience in searching for electronic evidence, I  
23 believe that if digital devices are found on the SUBJECT PREMISES, there is probable  
24 cause to believe that the items set forth in Attachment B will be stored in those digital  
25 devices for a number of reasons, including but not limited to the following:

26 a. Once created, electronically stored information ("ESI") can be stored  
27 for years in very little space and at little or no cost. A great deal of ESI is created, and  
28 stored, moreover, even without a conscious act on the part of the device operator. For

1 example, files that have been viewed via the Internet are sometimes automatically  
2 downloaded into a temporary Internet directory or “cache,” without the knowledge of the  
3 device user. The browser often maintains a fixed amount of hard drive space devoted to  
4 these files, and the files are only overwritten as they are replaced with more recently  
5 viewed Internet pages or if a user takes steps to delete them. This ESI may include  
6 relevant and significant evidence regarding criminal activities, but also, and just as  
7 important, may include evidence of the identity of the device user, and when and how the  
8 device was used. Most often, some affirmative action is necessary to delete ESI. Even  
9 when such action has been deliberately taken, ESI can often be recovered, months or even  
10 years later, using forensic tools.

11           b. Wholly apart from data created directly (or indirectly) by user-  
12 generated files, digital devices – in particular, a computer’s internal hard drive – contain  
13 electronic evidence of how a digital device has been used, what it has been used for, and  
14 who has used it. This evidence can take the form of operating system configurations,  
15 artifacts from operating systems or application operations, file system data structures, and  
16 virtual memory “swap” or paging files. Computer users typically do not erase or delete  
17 this evidence, because special software is often required for that task. However, it is  
18 technically possible for a user to use such software to delete this type of information -  
19 and, the use of such special software may itself result in ESI that is relevant to the  
20 criminal investigation.

21           45. In addition, based on my training and experience and that of other agents  
22 who have specialized training and experience in searching for electronic evidence, I know  
23 that in most cases it is impossible to successfully conduct a complete, accurate, and  
24 reliable search for electronic evidence stored on a digital device during the physical  
25 search of a search site for a number of reasons, including but not limited to the following:

26           a. Technical Requirements: Searching digital devices for criminal  
27 evidence is a highly technical process requiring specific expertise and a properly  
28 controlled environment. The vast array of digital hardware and software available

1 requires even digital experts to specialize in particular systems and applications, so it is  
2 difficult to know before a search which expert is qualified to analyze the particular  
3 system(s) and electronic evidence found at a search site. As a result, it is not always  
4 possible to bring to the search site all of the necessary personnel, technical manuals, and  
5 specialized equipment to conduct a thorough search of every possible digital  
6 device/system present. In addition, electronic evidence search protocols are exacting  
7 scientific procedures designed to protect the integrity of the evidence and to recover even  
8 hidden, erased, compressed, password-protected, or encrypted files. Since ESI is  
9 extremely vulnerable to inadvertent or intentional modification or destruction (both from  
10 external sources or from destructive code embedded in the system such as a "booby  
11 trap"), a controlled environment is often essential to ensure its complete and accurate  
12 analysis.

13           b.     Volume of Evidence: The volume of data stored on many digital  
14 devices is typically so large that it is impossible to search for criminal evidence in a  
15 reasonable period of time during the execution of the physical search of a search site. A  
16 single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A  
17 single gigabyte of storage space, or 1,024 megabytes, is the equivalent of 500,000 double-  
18 spaced pages of text. Computer hard drives are now being sold for personal computers  
19 capable of storing up to two terabytes (2,048 gigabytes of data.) And, this data may be  
20 stored in a variety of formats or encrypted (several new commercially available operating  
21 systems provide for automatic encryption of data upon shutdown of the computer.)

22           c.     Search Techniques: Searching the ESI for the items described in  
23 Attachment B may require a range of data analysis techniques. In some cases, it is  
24 possible for agents and analysts to conduct carefully targeted searches that can locate  
25 evidence without requiring a time-consuming manual search through unrelated materials  
26 that may be commingled with criminal evidence. In other cases, however, such  
27 techniques may not yield the evidence described in the warrant, and law enforcement  
28 personnel with appropriate expertise may need to conduct more extensive searches, such

1 as scanning areas of the disk not allocated to listed files, or peruse every file briefly to  
2 determine whether it falls within the scope of the warrant. These methodologies,  
3 techniques and protocols may include the use of a "hash value" library to exclude normal  
4 operating system files that do not need to be further searched.

5 46. In accordance with the information in this affidavit, law enforcement  
6 personnel will execute the search of digital devices seized pursuant to this warrant as  
7 follows:

8 a. Upon securing the search site, the search team will conduct an initial  
9 review of any digital devices/systems to determine whether the ESI contained therein can  
10 be searched and/or duplicated on site in a reasonable amount of time and without  
11 jeopardizing the ability to accurately preserve the data.

12 b. If based on their training and experience, and the resources available  
13 to them at the search site, the search team determines it is not practical to make an on-site  
14 search, or to make an on-site copy of the ESI within a reasonable amount of time and  
15 without jeopardizing the ability to accurately preserve the data, then the digital devices  
16 will be seized and transported to an appropriate law enforcement laboratory for review  
17 and to be forensically copied ("imaged,") as appropriate.

18 c. In order to examine the ESI in a forensically sound manner, law  
19 enforcement personnel with appropriate expertise will produce a complete forensic  
20 image, if possible and appropriate, of any digital device that is found to contain data or  
21 items that fall within the scope of Attachment B of this Affidavit. In addition,  
22 appropriately trained personnel may search for and attempt to recover deleted, hidden, or  
23 encrypted data to determine whether the data fall within the list of items to be seized  
24 pursuant to the warrant. In order to search fully for the items identified in the warrant,  
25 law enforcement personnel may then examine all of the data contained in the forensic  
26 image/s and/or on the digital devices to view their precise contents and determine whether  
27 the data fall within the list of items to be seized pursuant to the warrant.  
28

1           d.     The search techniques that will be used will be only those  
2 methodologies, techniques and protocols as may reasonably be expected to find, identify,  
3 segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to  
4 this affidavit.

5           e.     If, after conducting its examination, law enforcement personnel  
6 determine that any digital device is an instrumentality of the criminal offenses referenced  
7 above, the government may retain that device during the pendency of the case as  
8 necessary to, among other things, preserve the instrumentality evidence for trial, ensure  
9 the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel  
10 determine that a device was not an instrumentality of the criminal offenses referenced  
11 above, it shall be returned to the person/entity from whom it was seized within 90 days of  
12 the issuance of the warrant, unless the government seeks and obtains authorization from  
13 the court for its retention.

14           f.     Unless the government seeks an additional order of authorization  
15 from any Magistrate Judge in the District, the government will return any digital device  
16 that has been forensically copied, that is not an instrumentality of the crime, and that may  
17 be lawfully possessed by the person/entity from whom it was seized, to the person/entity  
18 from whom it was seized within 90 days of seizure.

19           g.     If, in the course of their efforts to search the subject digital devices,  
20 law enforcement agents or analysts discover items outside of the scope of the warrant that  
21 are evidence of other crimes, that data/evidence will not be used in any way unless it is  
22 first presented to a Magistrate Judge of this District and a new warrant is obtained to seize  
23 that data, and/or to search for other evidence related to it. In the event a new warrant is  
24 authorized, the government may make use of the data then seized in any lawful manner.

25           47.    In order to search for ESI that falls within the list of items to be seized  
26 pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and  
27 search the following items (heretofore and hereinafter referred to as "digital devices"),  
28 subject to the procedures set forth above:

1           a.     Any digital device capable of being used to commit, further, or store  
2 evidence of the offense(s) listed above;

3           b.     Any digital device used to facilitate the transmission, creation,  
4 display, encoding or storage of data, including word processing equipment, modems,  
5 docking stations, monitors, printers, cameras, plotters, encryption devices, and optical  
6 scanners;

7           c.     Any magnetic, electronic or optical storage device capable of storing  
8 data, such as thumbdrives, memory sticks, CD-ROMs, CD-R, CD-RWs, DVDs, optical  
9 disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic  
10 dialers, electronic notebooks, personal digital assistants, floppy disks, hard disks, and  
11 tapes;

12           d.     Any documentation, operating logs and reference manuals regarding  
13 the operation of the digital device, or software;

14           e.     Any applications, utility programs, compilers, interpreters, and other  
15 software used to facilitate direct or indirect communication with the device hardware, or  
16 ESI to be searched;

17           f.     Any physical keys, encryption devices, dongles and similar physical  
18 items that are necessary to gain access to the digital device, or ESI; and

19           g.     Any passwords, password files, test keys, encryption codes or other  
20 information necessary to access the digital device or ESI.

21 //

22  
23 //

24  
25 //



**CONCLUSION**

48. Based on the information in this Affidavit, I also believe that the digital device/s at the SUBJECT PREMISES are instrumentalities of crime and constitute the means by which violations of Title 18, United States Code, Sections 2319 and 2320 have been committed. Therefore, I believe that in addition to seizing the digital devices/systems to conduct a search of their contents as set forth herein, there is probable cause to seize those digital devices/system as instrumentalities of the criminal activity.

\_\_\_\_\_  
MICHAEL J. LARSON, Affiant  
Special Agent  
U.S. Immigration and Customs Enforcement

SUBSCRIBED and SWORN to before me this \_\_\_\_\_ day of February, 2011.

\_\_\_\_\_  
JAMES P. DONOHUE  
United States Magistrate Judge



## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of )  
(Briefly describe the property to be searched )  
or identify the person by name and address) )

Case No.

The residence located at 2305 Rucker Avenue, )  
Apt. 5, Everett, Washington 98201 )

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of Washington  
(identify the person or describe the property to be searched and give its location):

See Attachment A, attached hereto and incorporated herein

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before \_\_\_\_\_

(not to exceed 10 days)

- ☐ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge

JAMES P. DONOHUE

(name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for \_\_\_\_\_ days (not to exceed 30).

☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

Date and time issued: \_\_\_\_\_

Judge's signature

City and state: Seattle, Washington

JAMES P. DONOHUE, United States Magistrate Judge

Printed name and title

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

## **ATTACHMENT A**

### **SUBJECT PREMISES**

The SUBJECT PREMISES at 2305 Rucker Avenue, Apartment 5, Everett, Washington 98201 is more fully described as:

a two-story apartment building located near the intersection of Rucker Avenue and 23rd Street. The apartment building is tan or taupe in color; however, the lower level of the west side of the structure has a red brick facade. The west side of the house has a red entry door, and a single-car garage door. The number two thousand three hundred five (2305) is affixed to the brick facade to the left of the red entry door. On the north side of the building, there is a covered external stairway with entry doors on both the upper and lower levels. Apartment number five is located on the upper level of the building and the entry door to the unit is light green in color and marked with the number five.

## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

The items to be seized are the following items that constitute evidence, fruits, and instrumentalities of the crimes of Criminal Copyright Infringement in violation of Title 18, United States Code, Section 2319 and Trafficking in Counterfeit Goods in violation of Title 18, United States Code, Section 2320.

1. The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed); photocopies or other photographic form; and electrical, electronic, digital and magnetic form (in storage on or in media such as tapes, cassettes, hard disks, floppy disks, diskettes, compact disks, CD-ROMs, DVDs, optical disks, printer buffers, smartcards, electronic notebooks, memory cards, USB thumb drives, mobile or cellular phones, personal data assistants, or any other storage medium):

a. Counterfeit software and counterfeit software components including, boxes, labels, packaging, stickers, wrappers, emblems, medallions, documentation, license agreements, manuals, end user license agreements, and/or certificates of authenticity;

b. Records relating to the purchase and/or sale of software including invoices, purchase orders, correspondence with customers and/or suppliers of software, inventory lists, advertisements;

c. Records relating to the exporting or importing of computer software to or from countries other than the United States;

d. Records relating to licensing agreements for the distribution of computer software;

e. Shipping records including U.S. Mail, Federal Express, United Parcel Service, or any other common carrier;

f. Correspondence with Customs and Border Protection regarding any seizures of counterfeit software;

g. Correspondence with Microsoft Corporation or its affiliates regarding the distribution of counterfeit software;

h. Any books, papers, internet history, documents, pamphlets, or other

materials regarding counterfeit software;

i. Records related to the posting of advertisements for the sale of software on Internet classified advertising services such as eBid, Craigslist, Amazon.com and/or eBay, including drafts of advertisements, photographs of products advertised, account information, sales history, customer feedback reports, payment records, customer complaints, and correspondence with the classified advertisement service provider;

j. Any and all financial records present at the subject premises, including: checking and savings account bank statements; deposit or withdrawal records; safe deposit box records and keys; investment or brokerage account statements; cashier's check receipts; check books; receipts; wire transfer records; electronic funds transfer records; cancelled checks; credit card account statements and receipts; records of employment and earnings; bank loan or credit applications; business books and records; and telephone records;

k. Any and all evidence of dominion and control of the subject premises and/or any digital devices located at the subject premises;

l. Any and all United States currency, cashier's checks, money orders, travelers checks, and other monetary instruments;

2. Digital devices and/or their components, including:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data related to criminal copyright infringement and/or trafficking in counterfeit goods, including modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

d. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

e. Any physical keys, encryption devices, dongles and similar physical

items that are necessary to gain access to the computer equipment, storage devices or data; and

f. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

g. Evidence of who used, owned or controlled any seized digital device/s at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

h. Evidence of the attachment to the digital device/s of other storage devices or similar containers for electronic evidence;

i. Evidence of counter-forensics programs (and associated data) that are designed to eliminate data from a digital device;

j. Evidence of the times the digital device/s was used.

k. Any other ESI from the digital device/s necessary to understand how the digital device was used, the purpose for its use, who used it, and when.